Course Code: HYSPL03G

Course Title: Splunk Cluster Administration

Description:

This 3-virtual day course is for an experienced Splunk Enterprise administrator who is new to Splunk Clusters. The course provides the fundamental knowledge of deploying and managing Splunk Enterprise in a clustered environment. It covers installation, configuration, management, and monitoring of Splunk clusters.

Objectives:

- Large-scale Splunk Deployment Overview
- Identify factors affecting large-scale Splunk deployments
- Set up Splunk indexer clusters
- Deploy and configure a Splunk search head cluster
- Add new nodes into an existing cluster
- Decommission nodes from an existing cluster
- Deploy apps and configuration bundles in Splunk clusters
- Manage KV store collections and lookups in Splunk clusters
- Monitor and identify clustering issues with Monitoring Console
- Scale Splunk indexer cluster with SmartStore

Prerequisites:

Basic knowledge on Splunk fundamentals

Duration:

24 Hrs

Topics:

Module 1 – Splunk Troubleshooting Methods and Tools

- Deployment Design Factors
- How Splunk Enterprise can scale
- Splunk License Master

Module 2 – Singe-site Indexer Cluster

- How Splunk Single-Site Indexer Clusters Work
- Indexer Cluster Components and Terms
- Splunk single-site Indexer Cluster Configuration
- Splunk Indexer Cluster Log Channels

Module 3 – Multisite Indexer Cluster

- How Splunk Multisite Indexer Clusters Work

- Multisite Indexer Cluster Terms
- Multisite Indexer Cluster Configuration
- Optional Multisite Indexer Cluster Configurations

Module 4 – Indexer Cluster Management and Administration

- Peer Offline and Decommission
- Manager App Bundles
- Indexer Cluster Storage Utilization Options
- Site Mapping
- Monitoring Console for Indexer Cluster Environment
- Cluster Manager Redundancy

Module 5 – Forwarder Management

- Indexer Discovery
- Optional Indexer Discovery Configurations
- Volume-Based Forwarder Load Balancing

Module 6 – Search Head Cluster

- Search Head Cluster Architecture
- Search Head Cluster Configuration
- Captaincy Identification and Cluster Status
- Search Head Cluster Settings

Module 7 – Search Head Cluster Management

- Search Head Cluster Deployer
- Captaincy Transfer
- Search Head Member Addition and Decommissioning
- Monitoring Console for Search Head Cluster

Module 8 – KV Store Collection and Lookup Management

- KV Store Collection in Splunk Custers
- KV Store Monitoring with Monitoring Console

Module 9 – Introduction to Smart Store

- SmartStore Deployment Use Cases
- SmartStore Architecture Overview
- Enable SmartStore in Indexer Cluster
- Monitor SmartStore Status

Audience:

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification:

None